

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-243534

(43)Date of publication of application : 07.09.1999

(51)Int.Cl.

H04N 7/16  
H04N 7/167

(21)Application number : 10-043223

(71)Applicant : MATSUSHITA ELECTRIC IND CO  
LTD

(22)Date of filing : 25.02.1998

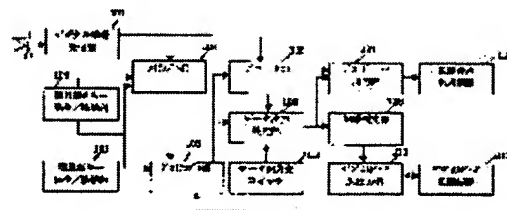
(72)Inventor : TAKAHASHI MASAYUKI

## (54) DIGITAL BROADCAST RECEPTION REPRODUCING APPARATUS

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To protect copying by preventing unauthorized viewing of a digital broadcast program by inhibiting recording of the program to various digital data storage devices.

**SOLUTION:** This apparatus is provided with a digital broadcast reception section 101 that receives a digital broadcast program, a device specific key generating/storage section 102 that generates a key specific to the device, a program-dependent key generating/storage section 103 that generates a key for each program and that stores each program key and a limit number of times of reproduction, a scramble section 104 that multiplexes each program key and video audio data and scrambles them by the use of a device specific key, and a descramble section 105 that descrambles each program key and the video audio data scrambled that come from a digital data input output section 110 by the use of the device specific key and that checks whether or not the data are reproduced by comparing the key with each program key from the program-dependent key generation/storage section 103. The digital data scrambled by the device specific key are given/outputted to/from a digital data storage device 113.



## LEGAL STATUS

[Date of request for examination]

08.03.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]	3428420
[Date of registration]	16.05.2003
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

Copyright (C); 1998,2003 Japan Patent Office

**Family list**

**4** family members for:

**JP11243534**

Derived from 3 applications.

**1 DIGITAL BROADCAST RECEPTION REPRODUCING APPARATUS**

Publication info: **JP3428420B2 B2** - 2003-07-22

**JP11243534 A** - 1999-09-07

**2 Digital broadcast receiving and reproducing apparatus**

Publication info: **SG70674 A1** - 2000-02-22

**3 Digital broadcast receiving and reproducing apparatus**

Publication info: **US6463152 B1** - 2002-10-08

---

Data supplied from the **esp@cenet** database - Worldwide

**Digital broadcast receiving and reproducing apparatus**

Patent Number: ☐ US6463152  
Publication date: 2002-10-08  
Inventor(s): TAKAHASHI MASAYUKI (JP)  
Applicant(s): MATSUSHITA ELECTRIC IND CO LTD (JP)  
Requested Patent: ☐ JP11243534  
Application Number: US19990257740 19990225  
Priority Number(s): JP19980043223 19980225  
IPC Classification: H04N7/167; H04K1/00  
EC Classification: H04N7/16E, H04N5/913  
Equivalents: JP3428420B2, SG70674

---

**Abstract**

---

A digital broadcast receiving and playing apparatus for receiving digital program data of pay broadcast, generating an apparatus individual key and a program key different in every program or every program division of a divided program in the receiving and playing apparatus, recording after scrambling the program data and program key by the apparatus individual key, controlling the number of times of display of program data received or played from memory device, thereby capable of prohibiting reproduction or display of program data more than the permitted number of times

---

Data supplied from the esp@cenet database - I2

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-243534

(43) 公開日 平成11年(1999) 9月7日

(51) Int.Cl.<sup>6</sup>

識別記号

F I

H 0 4 N 7/16  
7/167

H 0 4 N 7/16  
7/167

A  
Z

審査請求 未請求 請求項の数 3 O L (全 12 頁)

(21) 出願番号 特願平10-43223  
(22) 出願日 平成10年(1998) 2月25日

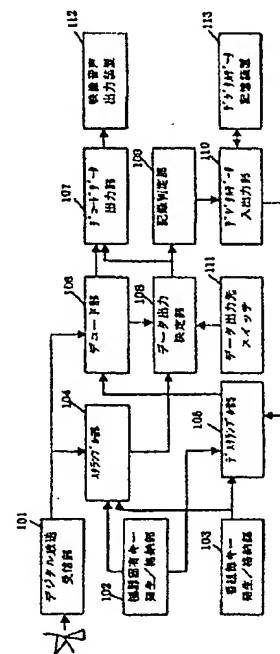
(71) 出願人 000005821  
松下電器産業株式会社  
大阪府門真市大字門真1006番地  
(72) 発明者 高橋 正之  
香川県高松市古新町8番地の1 松下電  
子工業株式会社内  
(74) 代理人 弁理士 滝本 智之 (外1名)

(54) 【発明の名称】 デジタル放送受信再生装置

(57) 【要約】

【課題】 デジタル放送の無断視聴や、各種デジタルデータ記憶装置への記録を防止して著作権の保護を可能にする。

【解決手段】 デジタル放送を受信するデジタル放送受信部101と、機器固有のキーを発生させる機器固有キー発生/格納部102と、番組毎のキーを発生させて番組毎のキーと再生制限回数を格納する番組毎キー発生/格納部103と、番組毎のキーと映像・音声データをマルチプレクスして装置固有のキーでスクランブルを行うスクランブル部104と、デジタルデータ入出力部110からのデータに対してスクランブルされた番組毎のキーと映像・音声データを装置固有のキーでデスクランブルして番組毎キー発生/格納部の番組毎のキーと比較して再生可能かをチェックするデスクランブル部105を設け、デジタルデータ記憶装置113と機器固有のキーでスクランブルされたデジタルデータの入出力を行う。



## 【特許請求の範囲】

【請求項1】 デジタル放送を受信してデジタルデータを復調し、そのデジタルデータからアナログ信号とコピープロテクション情報を取り出すデジタル放送受信再生装置において、前記受信再生装置固有のキーを発生させる機器固有キー発生／格納部と、放送受信番組に対応するキーを発生させるとともに前記コピープロテクション情報中の再生制限回数を格納する番組毎キー発生／格納部と、前記番組毎のキーと復調された前記デジタルデータをマルチプレクスして前記機器固有のキーでスクランブルを行うスクランブル部と、前記スクランブルされたデジタルデータを記録の可否を判定する記録判定部を介して記録するデジタルデータ記憶装置とを有し、前記記憶装置から再生されるスクランブルされたデジタルデータに対して前記装置固有のキーでデスクランブルされたデジタルデータと前記番組毎キーを抽出し、前記番組毎キー発生／格納部から出力される番組毎キーと再生制限回数を比較して、その比較結果に応じてデジタルデータを出力するとともに、各放送受信番組の再生毎に、前記番組毎キー発生／格納部に格納されているその放送番組に対応する前記再生制限回数を1つ減じることを特徴とするデジタル放送受信再生装置。

【請求項2】 番組毎キー発生／格納部の番組毎のキーを一つの番組内で予め定められた間隔毎に異なるキーを発生することを特徴とする請求項1に記載のデジタル放送受信再生装置。

【請求項3】 IDカード内に格納されたIDを元に機器固有のキーを発生させるとともに、番組毎のキーと前記デジタル放送受信時のコピープロテクション情報を前記IDカード内に格納することを特徴とする請求項1もしくは請求項2のいずれかに記載のデジタル放送受信再生装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、デジタル放送を無断で試聴したりコピーすることを防止して著作権を保護するようにしたデジタル出力機能を持ったデジタル放送受信再生装置に関する。

## 【0002】

【従来の技術】 従来、デジタル放送受信再生装置は、特開平9-93561号公報に記載されたものが知られている。

【0003】 図8は、従来のデジタル放送受信再生装置のブロックを示すものであり、コピープロテクションコントロールコードを格納し放送受信の可否を判定するスマートカード（IDカード）804と、番組データにかけられたスクランブルを解除するデスクランブル部802とデジタルデータとコピープロテクションコントロールコードを出力する記録及びデジタル出力制御部803からなるデジタル放送受信機801で構成され、デジ

タルデータを記録するデジタルVCR805とはデータ入出力ポートとテープからのデータ出力制御およびテープデータの消去制御を行う制御信号で接続される構成となっている。

## 【0004】

【発明が解決しようとする課題】 このように従来のデジタル放送受信再生装置においては、デジタルデータの記憶装置としてデジタルVCRのみならず磁気ディスク、追記型光磁気ディスク、リライタブル光磁気ディスクへの媒体展開が望まれ、有料放送においては契約者のみが再生可能で、ペイパービューは一度だけ再生可能という放送内容に対する著作権を守り、かつ、放送システムの根幹であるコピープロテクションコントロールコードを記憶媒体に記録しない耐ハッキング性のある有料放送、ペイパービューのデジタル放送受信、再生手段が要求されている。

## 【0005】

【課題を解決するための手段】 前記課題を解決するために、本発明のデジタル放送受信再生装置は、デジタル放送を受信してデジタルデータを復調し、そのデジタルデータからアナログ信号とコピープロテクション情報を取り出すデジタル放送受信再生装置において、前記受信再生装置固有のキーを発生させる機器固有キー発生／格納部と、放送受信番組に対応するキーを発生させるとともに前記コピープロテクション情報中の再生制限回数を格納する番組毎キー発生／格納部と、前記番組毎のキーと復調された前記デジタルデータをマルチプレクスして前記機器固有のキーでスクランブルを行うスクランブル部と、前記スクランブルされたデジタルデータを記録の可否を判定する記録判定部を介して記録するデジタルデータ記憶装置とを有し、前記記憶装置から再生されるスクランブルされたデジタルデータに対して前記装置固有のキーでデスクランブルされたデジタルデータと前記番組毎キーを抽出し、前記番組毎キー発生／格納部から出力される番組毎キーと再生制限回数を比較して、その比較結果に応じてデジタルデータを出力することを特徴としたものであり、スクランブルされた映像、音声データは、有料放送の場合受信した装置のみで指定回数再生可能で、ペイパービューの場合受信した装置で1回のみ再生可能で、放送システムの根幹であるコピープロテクションコントロールコードを外部に出力せず耐ハッキング性を有し、かつデジタルVCRのみならず磁気ディスク、追記型光磁気ディスク、リライタブル光磁気ディスクなどの媒体にも対応可能なデジタル放送受信再生装置が得られる。

## 【0006】

【発明の実施の形態】 本発明の請求項1に記載のデジタル放送受信再生装置は、デジタル放送を受信してデジタルデータを復調し、そのデジタルデータからアナログ信号とコピープロテクション情報を取り出すデジタル放送

受信再生装置において、前記受信再生装置固有のキーを発生させる機器固有キー発生／格納部と、放送受信番組に対応するキーを発生させるとともに前記コピープロテクション情報中の再生制限回数を格納する番組毎キー発生／格納部と、前記番組毎のキーと復調された前記デジタルデータをマルチプレクスして前記機器固有のキーでスクランブルを行うスクランブル部と、前記スクランブルされたデジタルデータを記録の可否を判定する記録判定部を介して記録するデジタルデータ記憶装置とを有し、前記記憶装置から再生されるスクランブルされたデジタルデータに対して前記装置固有のキーでデスクランブルされたデジタルデータと前記番組毎キーを抽出し、前記番組毎キー発生／格納部から出力される番組毎キーと再生制限回数を比較して、その比較結果に応じてデジタルデータを出力するとともに、各放送受信番組の再生毎に、前記番組毎キー発生／格納部に格納されているその放送番組に対応する前記再生制限回数を1つ減じること特徴としたものであり、デジタルデータ入出力部からのデータの再生において有料放送は受信された機器と同じ装置でのみ指定回数再生可能で、かつペーパービューの放送に対してデコードデータ出力部を介して番組を再生しなかった時のみデジタルデータ入出力部からのデータによる1度だけの再生を可能にすることができる。

【0007】請求項2に記載の発明は、請求項1において、番組毎キー発生／格納部の番組毎のキーを一つの番組内で予め定められた間隔毎に異なるキーを発生すること特徴としたものであり、再生回数の指定された放送における番組再生の部分再生に対しても指定回数だけ再生可能とすることができる。

【0008】請求項3に記載の発明は、請求項1あるいは請求項2において、IDカード内に格納されたIDを元に機器固有のキーを発生させるとともに、番組毎のキーと前記デジタル放送受信時のコピープロテクション情報を前記IDカード内に格納すること特徴としたものであり、デジタルデータ入出力部からのデータの再生がIDカードとセットの装置でのみ再生可能とすることができる。

【0009】(実施の形態1)以下に、本発明の請求項1及び請求項2に記載された発明の実施の形態について、図1、図2、図3、図4、図5および図6を用いて説明する。

【0010】図1において、デジタル放送受信部101では、デジタル放送を受信してコピープロテクション情報を取り出すとともに、デマルチプレクスして使用者指定の番組を取り出して必要ならコピープロテクション情報をもとにデスクランブルを行いデジタル音声、デジタル映像データを取り出す。デジタル放送受信部101で取り出された番組のデジタル音声、デジタル映像データは、デコード部106とスクランブル部104に送られる。デコード部106では、デジタル放送受信再生時に

はデジタル音声、デジタル映像データをデコードしてアナログ映像、アナログ音声に変換してデータ出力決定部108にデータを送る。

【0011】機器固有キー発生／格納部102では、受信したデジタルデータをデジタルデータ記憶装置113と入出力する時に行うスクランブル／デスクランブルのキーを発生、格納するものであり、機器毎に割り当てられた機器固有のキーを発生させる。番組毎キー発生／格納部103では、時間情報から番組毎に異なるキーを発生し、デジタル放送受信部101で受信したコピープロテクション情報の再生制限回数を格納する。

【0012】スクランブル部104では、デジタル放送受信部101から送られてくるデジタル音声、デジタル映像データと番組毎キー発生／格納部103から送られる番組毎キーをマルチプレクスし、機器固有キー発生／格納部102からのスクランブルキーでスクランブルをかけてデータ出力決定部108へデジタルデータを転送する。データ出力先スイッチ111では、使用者がデータの出力先をデコードデータ出力のみ、デジタルデータ出力のみ、両方の3つのいずれか1つを指定する。データ出力決定部108では、データ出力先スイッチ111がデコードデータ出力のみもしくはデコードデータとデジタルデータの両方に指定される時、デコードデータをデコードデータ出力部107へ転送する。また、データ出力決定部108では、データ出力先スイッチ111がデジタルデータ出力のみもしくはデコードデータとデジタルデータの両方に指定される時、デジタルデータを記録判定部109へ転送する。

【0013】記録判定部109では、デジタル放送受信部101で受信したコピープロテクション情報と、データ出力決定部108で指定されたデータ出力先情報をもとに記録可否の判定を行い、記録可能であればデジタルデータをデジタルデータ入出力部110へ転送する。デコードデータ出力部107では、アナログデータに対してアナログコピープロテクションである世代管理情報、マクロビジョンに代表されるプロテクションを付加してアナログ音声、アナログ映像をそれぞれアナログ音声端子、アナログ映像端子より映像音声出力装置112へ出力する。デジタルデータ入出力部110では、記録判定部109から送られるデジタルデータをデジタル入出力部110の出力端子(図示せず)からデジタルデータ記憶装置113へ出力する。また、デジタルデータ入出力部110では、デジタルデータ記憶装置113からの再生時はデジタルデータをデスクランブル部105へ転送する。

【0014】デスクランブル部105では、デジタルデータ入出力部110から送られてくるデジタルデータを機器固有キー発生／格納部102からのデスクランブルキーでデスクランブルを行い番組毎キーとデジタル音声、デジタル映像データを取り出すとともに、デジタル

データから取り出した番組毎キーと、番組毎キー発生／格納部103から送られる番組毎キーと再生制限回数を比較して再生の可否を決定して再生可能であるならばデジタルデータをデコード部106へ転送する。デコード部106では、デジタルデータ記憶装置113からの再生時にはデジタルデータをデコードしてアナログ映像、アナログ音声に変換してデコードデータ出力部107にデータを送る。

【0015】デジタル放送受信部101で受信したデジタルデータのデジタルデータ入出力部110からのデジタル出力可否判定の手順を、図2を用いて説明する。

【0016】図2において、ステップ201では、デジタル放送受信部101で抽出したコピープロテクション情報をもとに受信したデジタルデータが有料放送かチェックして、無料放送の場合はデジタルデータ出力可能と判断し、有料放送の場合はステップ202にて再生制限回数をチェックする。ステップ202で、デジタル放送受信部101で抽出したコピープロテクション情報をもとに再生制限回数があるかチェックし、再生制限回数がない場合はステップ203にて番組毎キーにゼロを、スクランブルキーに機器固有のキーを設定し、再生制限回数がある場合はステップ204にて番組毎キーに現在の年月日時分秒を設定するとともに、制限回数にコピープロテクション情報の制限回数を設定し、かつスクランブルキーに機器固有のキーの補数を設定して、次のスクランブル・マルチプレクス処理部205に手順を移す。

【0017】ステップ205のスクランブル・マルチプレクス処理では、番組毎キーとデジタル放送受信部101で受信したデジタルデータをマルチプレクスしてスクランブルキーでスクランブルをかけ、ステップ206のデータ出力先チェックを行う。ステップ206のデータ出力先チェックでは、データ出力先スイッチ111をチェックして出力先がデコードデータのみの場合はデジタルデータ出力なしと判断し、出力先がデジタルデータのみ場合はステップ207でデジタルデータ再生回数設定処理で現在再生回数に1を設定し、出力先がデコードデータ・デジタルデータ両方の場合はステップ208でデータ再生回数処理で現在再生回数に2を設定し、次のステップ209のデジタルデータ出力チェックに手順を移す。

【0018】ステップ209では、現在再生回数が制限回数以下もしくは番組毎キーがゼロの場合はステップ210の制限回数更新処理に移り、現在再生回数が制限回数より大きくかつ番組毎キーがゼロでない場合はデジタルデータ出力不可と判断処理する。ステップ210の制限回数更新処理では、制限回数から現在再生回数を減じたものを制限回数として更新し、デジタルデータ出力可能と判断処理する。

【0019】再生制限回数がある場合の番組毎キーの発生とスクランブル・マルチプレクス処理（ステップ20

5）での番組毎キーとデジタルデータのマルチプレクス処理について図3を用いて詳しく説明する。なお、番組キーは1番組を通して同じキーをもつ場合、1番組中の一定期間毎（例えば5分おき）に番組区間を発生して異なる番組キーを発生させる場合がある。

【0020】ステップ301では、デジタルデータが1つの番組区間の開始部分かをチェックして番組区間の開始区間であれば、番組毎キー設定ステップ302へ、そうでなければ番組区間チェックステップ303へ手順を移す。ステップ302では、番組毎キーとして年月日時分秒にゼロを付加したものを、番組毎エンドキーとして年月日時分秒の1を付加したものを発生させて番組区間チェックステップ303へ手順を移す。番組区間チェックステップ303では、デジタルデータが1つの番組区間のどの位置にあるかをチェックして番組の終了区間であれば番組毎エンドキーマルチプレクス処理ステップ304に手順を移し、番組の開始区間であれば番組毎キーマルチプレクス処理ステップ305に手順を移し、番組の途中区間であればスクランブル処理ステップ306に手順を移す。

【0021】番組毎エンドキーマルチプレクス処理ステップ304では、デジタルデータと番組毎エンドキーをマルチプレクスし、スクランブル処理ステップ306へ手順を移す。番組毎キーマルチプレクス処理ステップ305では、デジタルデータと番組毎キーをマルチプレクスし、処理をスクランブル処理ステップ306へ移す。

【0022】スクランブル処理ステップ306では、マルチプレクスされたデジタルデータ、番組毎キーと番組毎エンドキーをスクランブルキーと排他的論理オアを行ってスクランブルし、処理を記録最終データチェックステップ307へ手順を移す。記録最終データチェックステップ307では、番組の最終データかチェックして最終データであれば終了とし、そうでなければ処理を番組区間開始チェックステップ301へ手順を戻す。

【0023】スクランブル・マルチプレクス処理ステップ205およびスクランブル処理ステップ306でのデジタルデータへのスクランブルおよびマルチプレクスのデータ構造について図4を用いて詳しく説明する。

【0024】デジタル放送受信部101で取り出されるデジタルデータは、トランスポートデータ401の集まりからなっている。トランスポートデータ401の構造は、データの情報を格納するヘッダ402と実際の音声、映像データを格納するペイロード403からなっている。ヘッダ402には、スクランブルの情報を格納する2ビットのスクランブルビット404と独自のデータを入れることが可能な可変バイト長のプライベートデータ405がある。スクランブルのかけない番組、再生制限回数のない番組と再生制限回数のある番組を区別するため、スクランブルビット404にそれぞれ00、01、10を設定する。また、番組区間の切り替わりにお



いて番組毎キーもしくは番組毎エンドキーのデータの挿入が必要になるタイミングで、トランスポートデータ401を作成してプライベートデータ405に番組毎キー、番組毎エンドキーを入れる。スクランブル処理においては、トランスポートデータ401のスクランブルビット404より後ろのデータをスクランブル対象とする。

【0025】デジタルデータ入出力部110からのデジタルデータの再生可否判定手順を、図5を用いて説明する。スクランブルチェックステップ501では、デジタルデータ入出力部110からのデジタルデータをチェックしてスクランブルなしの場合は再生可能と判断し、スクランブル有で再生制限回数有りの場合は再生制限回数有りデスクランブルキー設定ステップ502に手順を移し、スクランブル有で再生制限回数無しの場合は再生制限回数無しデスクランブルキー設定ステップ503に手順を移す。再生制限回数有りの場合、デスクランブルキー設定ステップ502において、デスクランブルキーに機器固有のキーの補数を設定してデスクランブル・デマルチプレクス処理ステップ504へ手順を移す。再生制限回数無しの場合、デスクランブルキー設定ステップ503では、デスクランブルキーに機器固有のキーを設定してデスクランブル・デマルチプレクス処理ステップ504へ手順を移す。

【0026】デスクランブル・デマルチプレクス処理ステップ504では、デジタルデータに対してデスクランブルを行うとともに、デマルチプレクスして番組毎キーを取り出して番組毎キーチェックステップ505へ手順を移す。番組毎キーチェックステップ505では、番組毎キーがゼロかチェックしてゼロであれば再生制限回数なしなので再生可能と判断し、番組毎キーがゼロでなければ番組毎キー格納チェックステップ506へ手順を移す。番組毎キー格納チェックステップ506では、番組毎キーを番組毎キー発生/格納部103内の番組毎キーと比較して番組毎キーが一致すれば再生可能と判断し、そうでなければ再生不可と判断する。

【0027】次に、再生制限回数がある場合の、番組毎キー発生/格納部103内の制限回数と番組毎キーの更新処理について図6を用いて詳しく説明する。デスクランブル処理ステップ601では、デジタルデータをトランスポートデータ401単位でデスクランブルキーと排他論理オアしてデスクランブルして番組毎キー・番組毎エンドキー抽出ステップ602へ手順を移す。番組毎キー・番組毎エンドキー抽出ステップ602では、番組毎キー、番組毎エンドキーが格納されたトランスポートデータ401であればヘッダ402内のプライベートデータ405からキーを取り出してデータ種チェックステップ603へ手順を移す。データ種チェックステップ603では、処理中のトランスポートデータ401が番組エンドキーであれば制限回数デクリメント処理ステップ

605へ手順を移し、音声・映像データであればデコード部転送処理ステップ604へ手順を移し、番組毎キーであれば手順を再生最終データチェックステップ608へ手順を移す。

【0028】デコード部転送処理ステップ604では、トランスポートデータ401をデコード部106へ転送する。制限回数デクリメント処理ステップ605では、番組毎キー発生/格納部103内の制限回数を1つ減じて制限回数チェックステップ606へ手順を移す。制限回数チェックステップ606では、更新された番組毎キー発生/格納部103内の制限回数をチェックして制限回数がゼロより大きいならば再生最終データチェックステップ608へ手順を移し、制限回数がゼロならば番組毎キー削除ステップ607へ手順を移す。番組毎キー削除ステップ607では、番組毎キー発生/格納部103内から再生中の番組の番組キーを削除して次回以降再生不可とし、再生最終データチェックステップ608へ手順を移す。再生最終データチェックステップ608では、処理中のトランスポートデータ401が再生番組の最終データかチェックして最終であれば再生を終了し、そうでなければ手順をデスクランブル処理ステップ601へ手順を戻す。

【0029】(実施の形態2)以下に、本発明の請求項3に記載された発明の実施の形態について、図7を用いて説明する。

【0030】図7において、デジタル放送受信部101では、デジタル放送を受信してコピープロテクション情報を取り出すとともに、デマルチプレクスして使用者指定の番組を取り出して必要ならコピープロテクション情報をもとにデスクランブルを行いデジタル音声、デジタル映像データを取り出す。デジタル放送受信部101で取り出された番組のデジタル音声、デジタル映像データは、デコード部106とスクランブル部104に送られる。デコード部106では、デジタル放送受信再生時にはデジタル音声、デジタル映像データをデコードしてアナログ映像、アナログ音声に変換してデータ出力決定部108にデータを送る。

【0031】機器固有キー発生部701では、デジタルデータをデジタルデータ記憶装置113と入出力する時に行うスクランブル/デスクランブルのキーをIDカード(スマートカード)703内のIDを元に発生、たとえばIDとバイト毎に10101010と排他論理オアを取ってスクランブル/デスクランブルのキーを発生するものであり、機器毎に割り当てた機器個々に異なるキーを発生させる。番組毎キー発生部702では、時間情報から番組毎に異なるキーを発生し、番組毎キーとデジタル放送受信部101で受信したコピープロテクション情報の再生制限回数をスマートカード703内に格納する。スクランブル部104では、デジタル放送受信部101から送られてくるデジタル音声、デジタル映像データと番組

毎キー発生部702から送られる番組毎キーをマルチプレクスし、機器固有キー発生部701からのスクランブルキーでスクランブルをかけてデータ出力決定部108へデジタルデータを転送する。

【0032】データ出力先スイッチ111では、使用者がデータの出力先をデコードデータ出力のみ、デジタルデータ出力のみ、両方の3つのいずれか1つを指定する。データ出力決定部108では、データ出力先スイッチ111がデコードデータ出力のみもしくは両方に指定される時デコードデータをデコードデータ出力部107へ転送する。また、データ出力決定部108では、データ出力先スイッチ111がデジタルデータ出力のみもしくは両方に指定される時デジタルデータを記録判定部109へ転送する。記録判定部109では、デジタル放送受信部101で受信したコピープロテクション情報と、データ出力決定部108で指定されたデータ出力先情報をもとに記録可能の判定を行い、記録可能であればデジタルデータをデジタルデータ入出力部110へ転送する。

【0033】デコードデータ出力部107では、アナログデータに対してアナログコピープロテクションである世代管理情報、マクロビジョンに代表されるプロテクションを付加してアナログ音声、アナログ映像をそれぞれアナログ音声端子、アナログ映像端子より映像音声出力装置112へ出力する。

【0034】デジタルデータ入出力部110では、記録判定部109から送られるデジタルデータをデジタルデータ入出力部110の出力端子（図示せず）からデジタルデータ記憶装置113へ出力する。また、デジタルデータ入出力部110では、デジタルデータ記憶装置113からの再生時はデジタルデータをデスクランブル部105へ転送する。デスクランブル部105では、デジタルデータ入出力部110から送られてくるデジタルデータを機器固有キー発生部701からのデスクランブルキーでデスクランブルを行い番組毎キーとデジタル音声、デジタル映像データを取り出すとともに、デジタルデータから取り出した番組毎キーと、番組毎キー発生部702から送られる番組毎キーと再生制限回数を比較して再生の可否を決定して再生可能であるならばデジタルデータをデコード部106へ転送する。デコード部106では、デジタルデータ記憶装置113からの再生時にはデジタルデータをデコードしてアナログ映像、アナログ音声に変換してデコードデータ出力部107にデータを送る。

【0035】デジタルデータのデジタルデータ入出力部110からの出力可否判定手順、番組毎キー発生と番組毎キーとデジタルデータのマルチプレクス処理、デジタルデータへのスクランブルおよびマルチプレクスのデータ構造、デジタルデータ入出力部110からのデジタルデータの再生可否判定手順、再生時の制限回数と番組毎

キーの更新処理手順は、実施の形態1と同様である。

【0036】なお、以上の実施の形態1の説明では、番組毎キーを時間情報から設定する例で説明したが、その他記録の度にインクリメントするシーケンシャル値など再現性の無いキーが発生できれば同様に実施可能である。再生制限回数のある番組に対して機器固有のキーの補数をスクランブルキー、デスクランブルキーとする例で説明したが2の補数など機器固有のキーと異なる値で有れば同様に実施可能であり、再生回数制限の無いキーと同じ機器固有のキーそのものをスクランブルキー、デスクランブルキーとして使用しても本実施の形態よりは耐ハッキング性が弱くなるが実施可能である。

【0037】また、1番組中の5分おきに番組区間を発生させる例で説明したが、他の時間間隔や可変の時間間隔であっても同様に実施可能である。番組毎エンドキーと番組毎キーを時間情報にそれぞれ1あるいは0を付加して設定する例で説明したが、他のコードを付加するなど番組毎エンドキーと番組毎キーがセットで区別できれば同様に実施可能である。スクランブル処理においてデジタルデータをスクランブルキーと排他的論理オアを取る例で説明したが、他の論理演算やデータの入れ替えを行っても同様に実施可能である。スクランブルのかけない番組、再生制限回数のない番組と再生制限回数のある番組を区別するため、スクランブルビット404にそれぞれ00、01、10と設定する例で説明したが、区別がつくビットパターンの組み合わせであれば同様に実施可能であり、再生制限回数のない番組と再生制限回数のある番組のスクランブルキーを同じにした場合は再生制限回数のない番組と再生制限回数のある番組のスクランブルビット404の値を同じにしても同様に実施可能である。

【0038】スクランブルをかける位置を、トランスポートデータ401のスクランブルビット404より後ろとする例で説明したが、プライベートデータ405以降であれば同様に実施可能であり、ペイロード403だけをスクランブル対象とした場合は本実施の形態よりは耐ハッキング性が弱くなるが実施可能である。デジタルデータ記憶装置113へ送るデータ形式をトランスポートデータ401とする例で説明したが、トランスポートデータ401をもとにパケット、バックのデータ形式に変換してスクランブルを行っても同様に実施可能である。番組毎キー、番組毎エンドキーをマルチプレクスするときにトランスポートデータ401を新たに挿入する例で説明したが、音声・映像データのプライベートデータ405にそのまま入れても、分割して入れても同様に実施可能である。

【0039】実施の形態2の説明では、機器固有のキーをスマートカード703内のIDとバイト毎に10101010と排他的論理オアを取って求める例で説明したが、他の論理演算やデータの入れ替えを行っても1つのIDから

[0040]

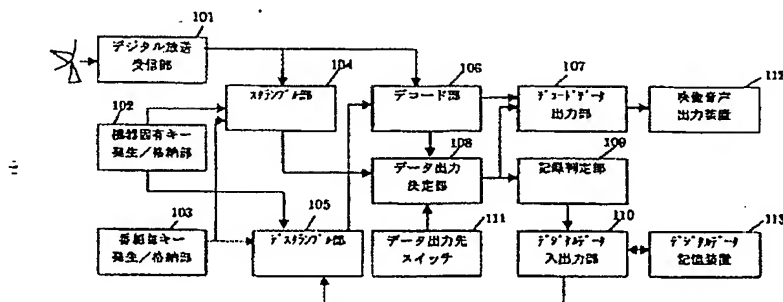
【図面の簡単な説明】

【図6】本発明の実施の形態における再生時の制限回数

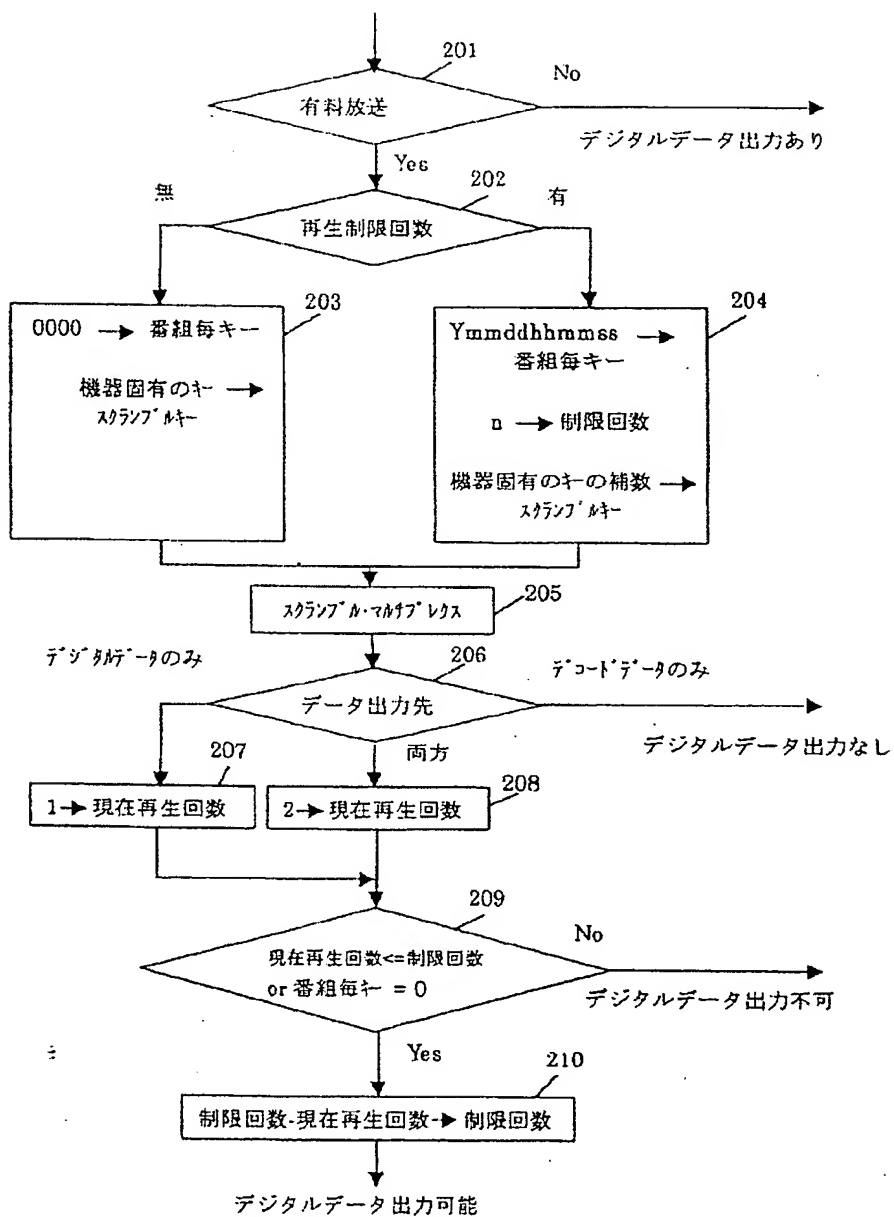
【符号の説明】

- 101 デジタル放送受信部
- 102 機器固有キー発生／格納部
- 103 番組毎キー発生／格納部
- 104 スクランブル部
- 105 デスクランブル部
- 106 デコード部
- 107 デコードデータ出力部
- 108 データ出力決定部
- 109 記録判定部
- 110 デジタルデータ入出力部
- 111 データ出力先スイッチ
- 112 映像音声出力装置
- 113 デジタルデータ記憶装置
- 401 トランスポートデータ
- 402 ヘッド
- 403 ベイロード
- 404 スクランブルビット
- 405 プライベートデータ
- 701 機器固有キー発生部
- 702 番組毎キー発生部
- 703 IDカード（スマートカード）

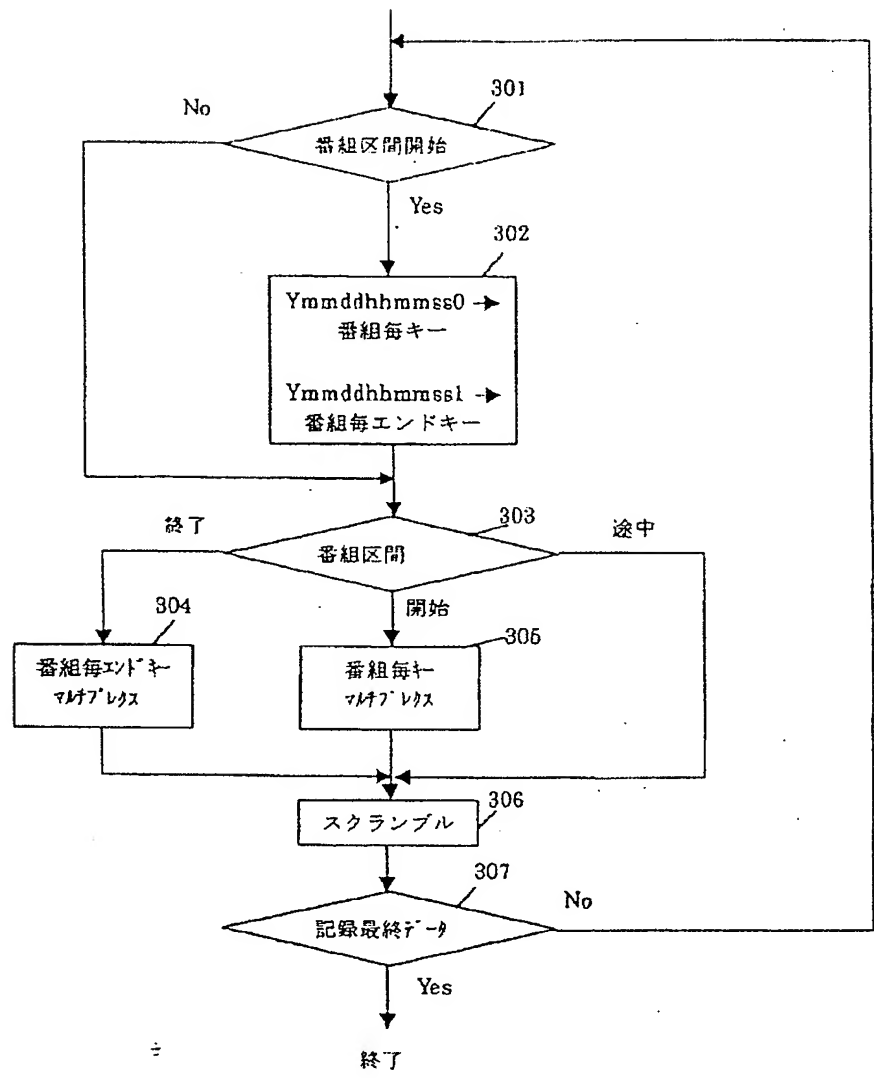
【图1】



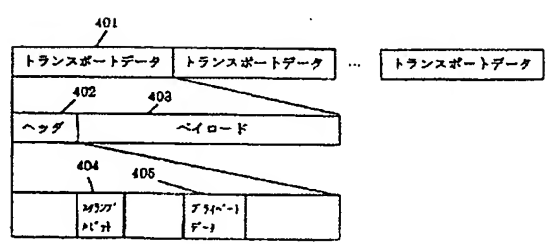
【図2】



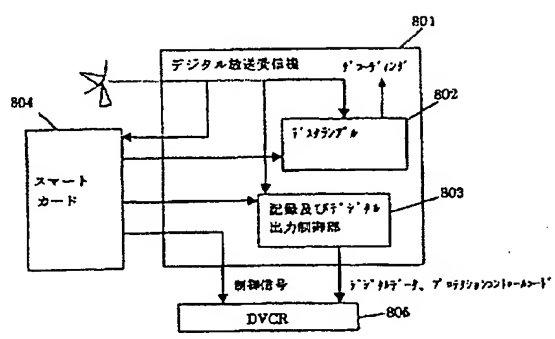
【図3】



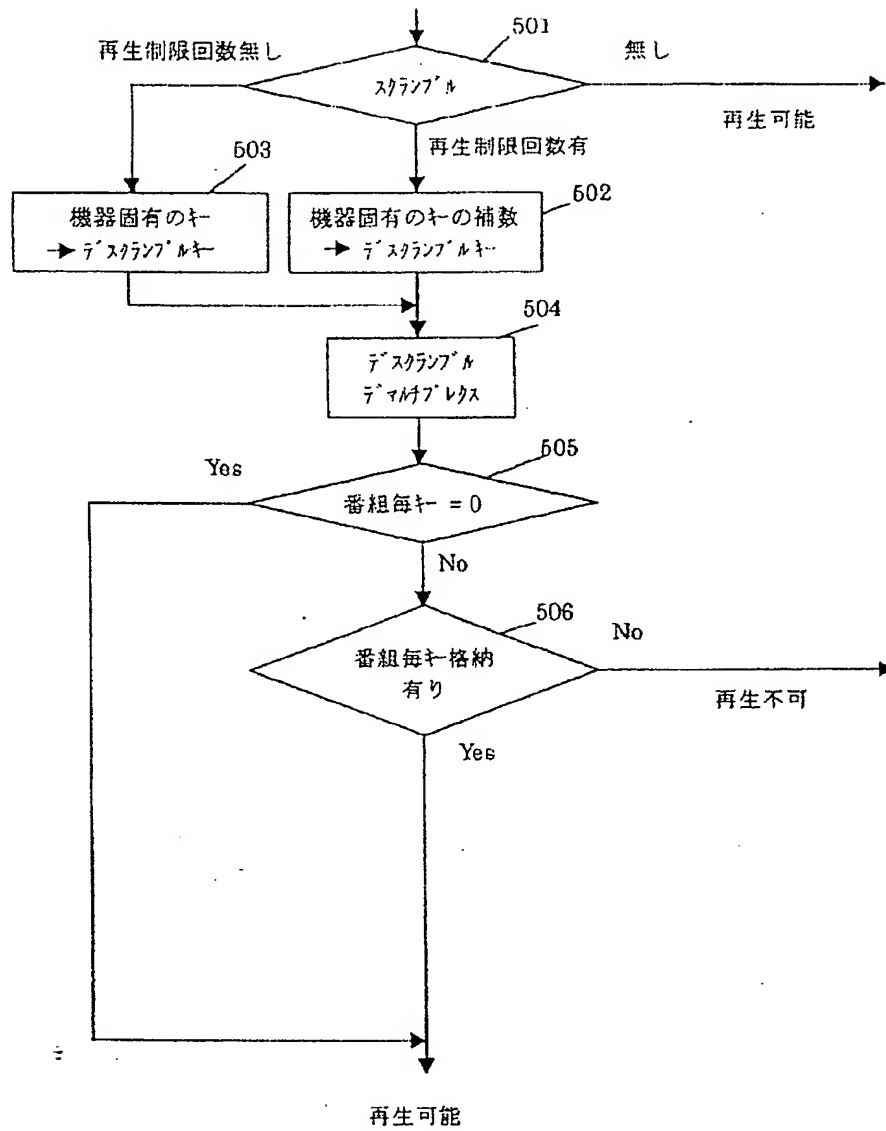
【図4】



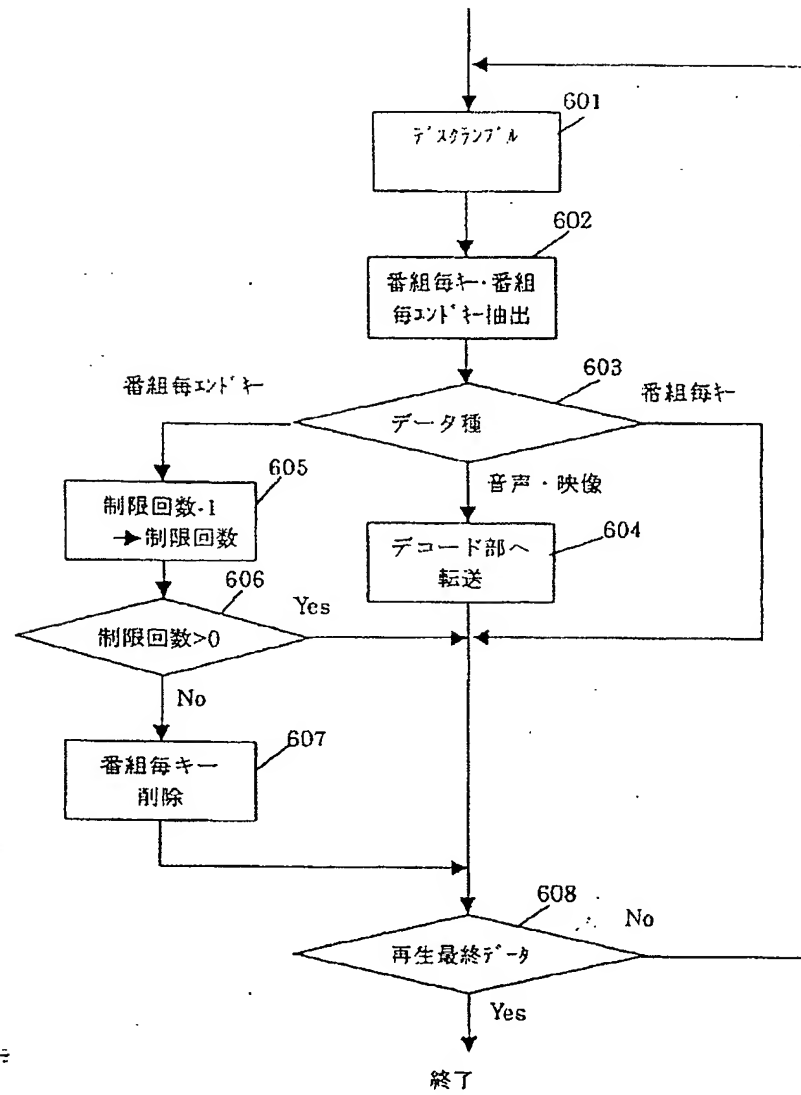
【図8】



【図5】



【図6】



【図7】

